SonicWall Detects, Reports Dramatic Rise in Fraudulent PDF Files in Q1 2019

Submitted by: SonicWall
Thursday, 18 April 2019

MILPITAS, Calif. — APRIL 18, 2019 — SonicWall Capture Labs threat researchers are reporting a substantial increase of fraudulent PDF files. This fraud campaign takes advantage of recipients' trust in PDF files as a "safe" file format that is widely used and relied upon for business operations.

"Increasingly, email, Office documents and now PDFs are the vehicle of choice for malware and fraud in the cyber landscape," said SonicWall President and CEO Bill Conner. "SonicWall Capture ATP with its RTDMI technology is at the forefront of catching new cyberattacks that elude traditional security sandbox technology. For example, in all of last year, our Capture ATP sandbox discovered more than 47,000 new attack variants in PDF files. This year, we've already seen that number rise significantly with over 73,000 PDF-based attacks discovered in March alone."

Last year, SonicWall Real-Time Deep Memory Inspection (RTDMI™) identified over 74,000 never-before-seen attacks, a number that has already been surpassed in the first quarter of 2019 with more than 173,000 new variants detected. In March, the company's patent-pending RTDMI technology identified over 83,000 unique, never-before-seen malicious events, of which over 67,000 were PDFs linked to scammers and more than 5,500 were PDFs with direct links to other malware.

Targets of the phishing style PDF scam campaigns typically receive malicious documents from "businesses" luring victims with attached PDF files that look deceivingly realistic with misleading links to fraudulent pages. The business offer within the PDF attachment is enticing to recipients, as it promises to be free and profitable with just the click of a link.

Most traditional security controls cannot identify and mitigate links to scams or malware hidden in PDF files, greatly increasing the success of the payload. This increase implies a growing, widespread and effective strategy against small- and medium-sized businesses, enterprises and government agencies.

RTDMI identifies and blocks malware that may not exhibit any detectable malicious behavior or hides its weaponry via encryption. By forcing malware to reveal its weaponry into memory, RTDMI detects and proactively stops mass-market, zero-day threats and unknown malware accurately utilizing real-time, memory-based inspection techniques. RTDMI also analyzes documents dynamically via proprietary exploit detection technology, along with static inspection, to detect many malicious document categories.

About SonicWall
SonicWall has been fighting the cybercriminal industry for over 27 years defending small and medium businesses, enterprises and government agencies worldwide. Backed by research from SonicWall Capture Labs, our award-winning, real-time breach detection and prevention solutions secure more than a million networks, and their emails, applications and data, in over 215 countries and territories. These organizations run more effectively and fear less about security. For more information, visit www.sonicwall.com (http://www.sonicwall.com/) or follow us on Twitter (https://twitter.com/SonicWall), LinkedIn (https://www.linkedin.com/company/SonicWall), Facebook (https://www.facebook.com/SonicWall) and Instagram (https://www.instagram.com/sonicwall_inc).

Contact
Elliot Harrison, Account Director, Positive Marketing
eharrison@positivemarketing.com
+44 (0)7763 683 055